**BUG REPORTS**

**Project-1(picoctf,** **Irish-Name-Repo 1)**

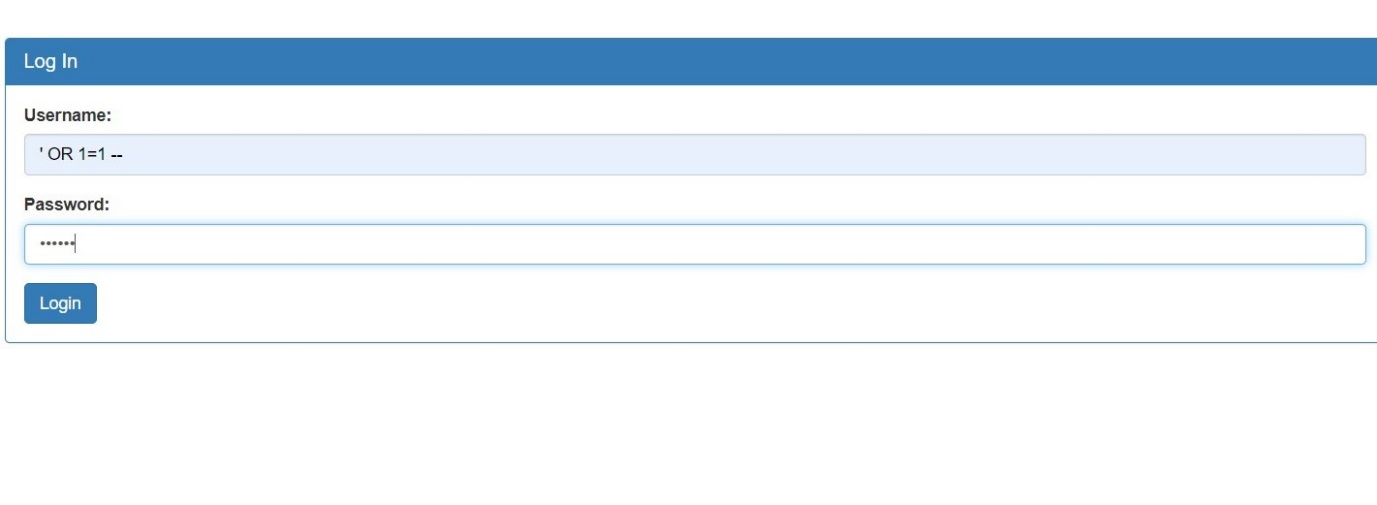
* **Title:** sql injection vulnerability in Irish-Name-Repo 1
* **Steps to reproduce:** 1)Go toIrish-Name-Repo 1 ctf challenge

2) Go to Admin Login panel

3) Enter the payload (‘ OR 1=1 --) in the place of the username

4)Enter anything in the place of password and press submit

5)As soon as you enter it will redirect you to the Admin Dashboard

* **Payload:** ‘ OR 1=1 --
* **Impact:** This vulnerability leads the attacker to access the database from admin account which may lead to Data Breach or database takeover
* **Proof of Concept:** 

**Project2(picoctf,** **JaWT Scratchpad)**

* **Title:** Login information saved in JWT token
* **Description of vulnerability:** In this type of vulnerability all the login details are saved in the jwt token and by changing
* **Steps to Reproduce:** 1) Enter any name in scratchpad

2)Go to inspect🡪Application🡪cookies🡪jwt and copy the token

3)Go to the website **jwt.io** and paste the key

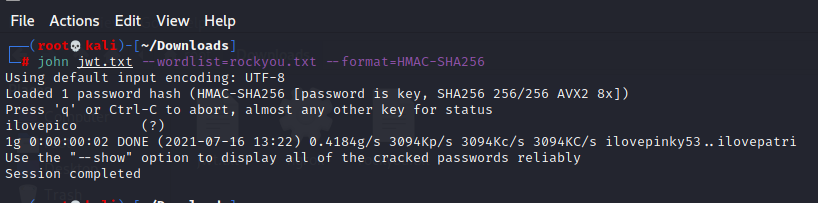
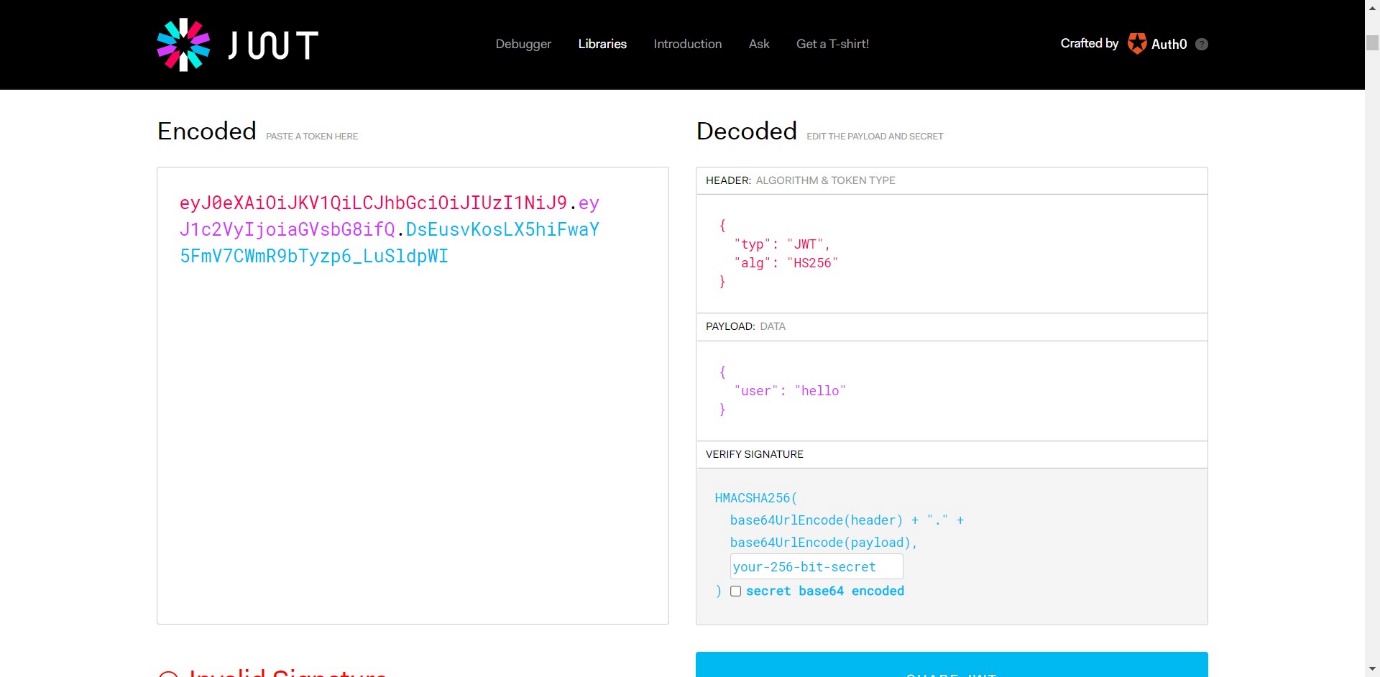
open the terminal and enter the command

**John jwt.txt --wordlist=rockyou.txt --format=HMAC-SHA256**

5)Now you will get the secret key paste it in the jwt.io and change name you entered to admin

6)Copy the modified jwt token and paste it in the place of websites jwt token and refresh the page

7)Now you will get logged in to admin account

* **Impact:** Access to the admin panel
* **Proof of concept:**

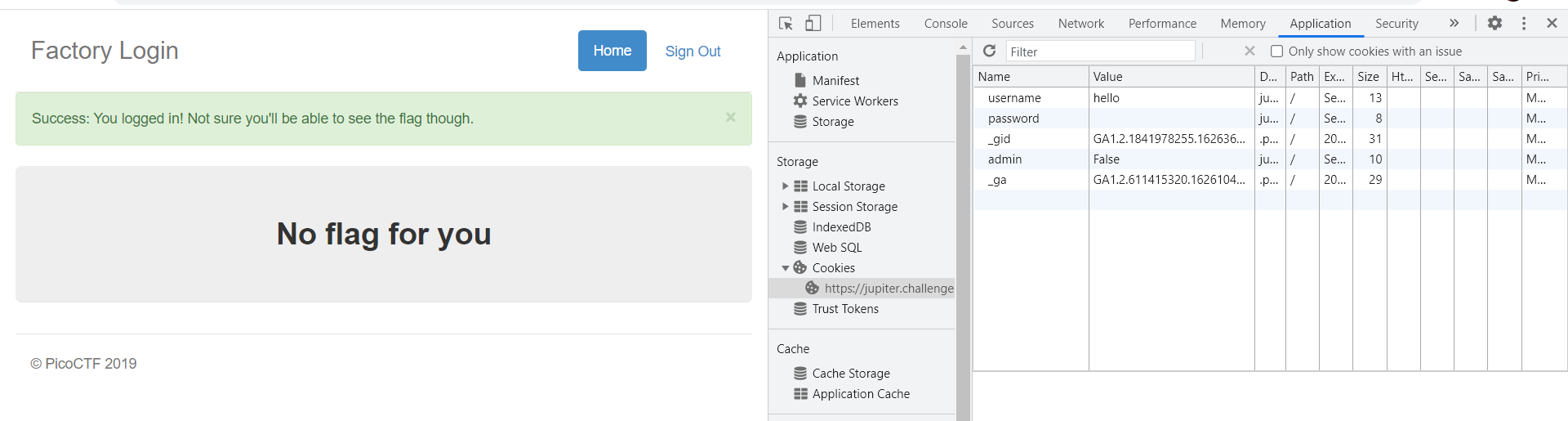
**Project3(picoctf,** **logon)**

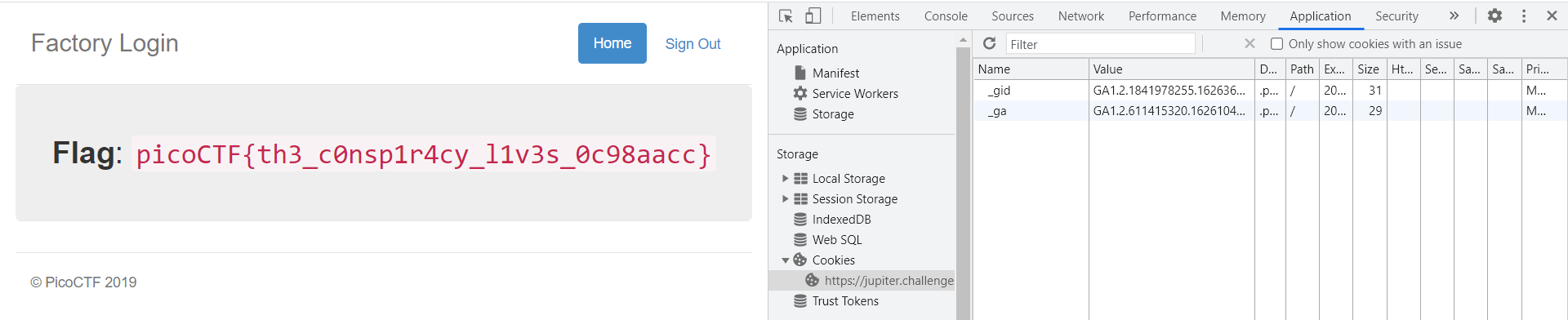
* **Title:** Login information saved in client side
* **Steps to reproduce:** 1) Go to factory login page

2)Enter any login detail and press submit

3)Right click on inspect element 🡪Application🡪cookies🡪admin and change False to true

4)Now you logged in to the admin account

* **Impact:** Access to admin login page
* **Proof of concept:** 

****